타입 II ONB를 이용한 $GF(2^m)$상의 곱셈에 대한 낮은 복잡도와 작은 지연시간을 가지는 시스톨릭 어레이

정회원 권 순 학*, 준회원 권 윤 기*, 정회원 김 창 훈**, 홍 춘 표***

A Low Complexity and A Low Latency Systolic Arrays for Multiplication in $GF(2^m)$ Using An Optimal Normal Basis of Type II

Soonhak Kwon* ***Regular Member***, Yun Ki Kwon* ***Associate Member***,
Chang Hoon Kim**, Chun Pyo Hong*** ***Regular Members***

요 약

타입 II ONB(optimal normal basis)의 자기쌍대성(self duality)을 이용하여 낮은 하드웨어 복잡도와 작은 지연시간을 가지는 $GF(2^m)$상의 비트 패러럴, 시리얼 시스톨릭 어레이를 제안하였다. 제안된 곱셈기는 $m+1$의 지연시간을 가지며 각 셀은 5개의 래치(플립-플롭)로 구성된다. 제안된 어레이는 다른 어레이와 비교하여 공간 복잡도와 지연시간을 줄임을 알 수 있다.

Key Words : ONB, Finite Field, Multiplication, Systolic Array

ABSTRACT

Using the self duality of an optimal normal basis(ONB) of type II, we present a bit parallel and bit serial systolic arrays over $GF(2^m)$ which has a low hardware complexity and a low latency. We show that our multiplier has a latency $m+1$ and the basic cell of our circuit design needs 5 latches (flip-flops). Comparing with other arrays of the same kinds, we find that our array has significantly reduced latency and hardware complexity.

Ⅰ. 서 론

유한체의 산술 연산, 특히 유한체 곱셈은 암호학과 코딩 이론 분야에서 다양하게 적용되고 있다. 그러므로 유한체 곱셈기의 효율적인 구조가 요구된다. 좋은 곱셈 알고리즘은 주어진 유한체상에서 기저의 선택에 좌우된다. 일반적으로 기저는 다항식기저, 쌍대기저, 정규기저, 이 세 가지 형태가 있다. 암호학과 코딩 이론적인 용도로 사용되는 몇 가지 대표적인 곱셈기는 쌍대기저를 이용하는 Berlekamp 비트 시리얼 곱셈기[1,2]와 정규기저를 이용한 Massey-Omura 타입의 비트 패러럴 곱셈기[4,5,17,18]가 있다. 앞에서 언급된 곱셈기들을 비롯한 다른 기존의 곱셈기들은 몇 개의 단점을 갖는다. 예를 들어, 그것

※ 이 논문은 2005년도 정부(교육인적자원부)의 재원으로 한국학술진흥재단의 지원을 받아 수행된 연구임(KRF-2005-041-C00004).
* 성균관대학교 수학과(shkwon@skku.edu, drmath@skku.edu)
** 대구대학교 컴퓨터IT공학부(chkim@dsp.daegu.ac.kr)
*** 대구대학교 정보통신공학부(cphong@daegu.ac.kr)
논문번호 : KICS2007-04-176, 접수일자 : 2007년 3월 23일, 최종논문접수일자 : 2007년 11월 20일

들은 불규칙한 회로 구조를 갖는다. 다시 말해, 곱셈 알고리즘이 각 m에 대해 기본적으로 같을지라도 그것들의 하드웨어 구조는 $GF(2^m)$상에서 m의 여러 가지 선택에 대해 상당히 달라질 수 있다. 게다가 m을 큰 수로 선택한다면, 전달 지연시간 또한 증가한다. 그래서 실행의 저하는 피할 수 없다.

시스톨릭 곱셈기는 위의 문제에 영향을 받지 않는다. 그것은 같은 회로 구조를 갖는 각각의 반복되는 기본 셀의 개수로 구성되는 일정한 구조를 갖는다. 그래서 시스톨릭 곱셈기의 전체 구조는 같고 $GF(2^m)$상에서 특정한 m의 선택에 의존하지 않는다. 더욱이 각 기본 셀이 이웃되는 셀에 연결될 뿐이므로 신호는 빠른 클럭(clock) 속도로 전파될 수 있다. 다항식기저[7,8,10,11,12,13,15]와 쌍대기저[9]를 이용한 시스톨릭 곱셈기는 잘 알려져 있다. [8]의 비트 패러럴 곱셈기는 [7,9,10]에서 제안된 곱셈기와 비슷하거나 좀 더 긴 지연시간을 갖는다. 그러나 [7,9,10]의 곱셈기가 단방향 자료 흐름을 갖는 반면 [8]에서 제안된 곱셈기는 양방향 자료 흐름을 갖는다. [10]에서 제안된 비트 패러럴 시스톨릭 곱셈기는 AOP(all one polynomial) 기저를 사용한다. 이 AOP 곱셈기는 다른 곱셈기와 비교했을 때 낮은 셀 복잡도와 높은 처리량을 갖는다. 그러나 100보다 작은 m에 대해서 m이 2, 4, 10, 12, 18, 28, 36, 52, 58, 60, 66, 82 일 때 기약다항식으로서의 AOP를 만족하므로, 특정한 m에 대해서만 $GF(2^m)$상의 AOP 곱셈기를 구현할 수 있다. 반면에 다항식기저를 이용한 곱셈기는 $GF(2^m)$상의 모든 m에 대해 구현할 수 있다.

본 논문에서는 $GF(2^m)$상에서 타입 II ONB(optimal normal basis : 최적정규기저)를 이용한 곱셈에 대한 새로운 비트 패러럴 시스톨릭 어레이와 비트 시리얼 시스톨릭 어레이를 제안한다. 또한, 제안된 비트 패러럴 시스톨릭 어레이와 비트 시리얼 시스톨릭 어레이가 [7,8,9,11]에서 제안된 다른 시스톨릭 곱셈기와 비교했을 때 낮은 하드웨어 복잡도를 가짐을 보인다. [10]에서 제안된 AOP 기저를 이용한 비트 패러럴 시스톨릭 곱셈기가 우리가 제안한 곱셈기보다 낮은 하드웨어 복잡도를 가지지만, 제안된 곱셈기는 더 많은 경우의 유한체에 적용된다. 또한 제안된 곱셈기는 지연시간이 $3m$을 가지는 같은 타입의 다른 곱셈기에 비해 $m+1$로서 작은 지연시간을 가진다.

Ⅱ. 정규기저 및 타입 II ONB

2^m개의 원소를 가지는 유한체를 $GF(2^m)$이라 하자. $GF(2^m)$은 $GF(2)$상의 m차원 벡터 공간이다. 이 장에서는 기본적인 유한체 산술 연산에 대해 주로 설명한다.

정의 1. $GF(2^m)$상의 두 기저 $\{\alpha_1,\alpha_2,\cdots,\alpha_m\}$과 $\{\beta_1,\beta_2,\cdots,\beta_m\}$이 다음을 만족시킬 때, 기저 $\{\beta_1,\beta_2,\cdots,\beta_m\}$을 $\{\alpha_1,\alpha_2,\cdots,\alpha_m\}$의 쌍대기저(dual basis)라 한다. :

모든 $1\le i, j\le m$에 대해,

$$Tr(\alpha_i\beta_j)=\delta_{ij},\quad \delta_{ij}=\begin{cases}1, & i=j\\ 0, & i\neq j\end{cases}$$

이고, 여기서 대각합(trace) 함수 $Tr: GF(2^m)\rightarrow GF(2)$, $Tr(\alpha)=\alpha+\alpha^2+\cdots+\alpha^{2^{m-1}}$이다. $Tr(\alpha_i\alpha_j)=\delta_{ij}$ 이면 기저 $\{\alpha_1,\alpha_2,\cdots,\alpha_m\}$을 자기쌍대기저(self dual basis)라 한다.

정의 2. $GF(2)$상에서 $GF(2^m)$의 $\{\alpha,\alpha^2,\cdots,\alpha^{2^{m-1}}\}$ 형태의 기저를 $GF(2^m)$에 대한 정규기저(normal basis)라 한다.

$GF(2^m)$상의 정규기저는 모든 m에 대해 존재한다는 것이 알려져 있다[6]. 특히 [4,6]에서 자세히 언급된 ONB 타입에 대해 알아보자.

정리 1. $2m+1=p$가 소수이고 2^m개의 원소를 가지는 유한체를 $GF(2^m)$이라 하자. 다음 조건

(*) 2는 mod p에 대해 원시근이거나

(**) -1는 mod p에 대해 이차 비잉여(quadratic non-residue)이고 2는 mod p에 대해 이차 잉여류(quadratic residues)를 생성한다.

을 가정하자. 그러면, β가 $GF(2^{2m})$상에서 p번째 원시근일 때, $\alpha=\beta+\beta^{-1}$라 하면, $\alpha\in GF(2^m)$이고 $\{\alpha,\alpha^2,\cdots,\alpha^{2^{m-1}}\}$은 $GF(2)$상의 기저이다.

정의 3. 정리 1에서의 정규기저를 타입 II ONB(optimal normal basis : 최적정규기저)라 한다.

정리 1의 가정을 사용하면

$$\alpha^{2^s} = (\beta+\beta^{-1})^{2^s} = \beta^{2^s}+\beta^{-2^s} = \beta^t+\beta^{-t},$$
$$0<t<p=2m+1, 2^s \equiv t \pmod p$$

을 쉽게 얻는다. 게다가, $m+1 \le t \le 2m$일 때 t를 p-t로 바꾸면, $\{\alpha,\alpha^2,\cdots,\alpha^{2^{m-1}}\}$과 $\{\beta+\beta^{-1},\beta^2+\beta^{-2},\cdots,\beta^m+\beta^{-m}\}$는 같은 집합임을 알 수 있다. 즉, α^{2^s} $(0 \le s \le m-1)$은 $\beta^s+\beta^{-s}$ $(1 \le s \le m)$의 치환(permutation)이다. 제안하는 비트 시리얼 곱셈기 구조에서 다음에 언급할 타입 II ONB의 자기쌍대성(self duality)이 필요하다. Gauss 주기의 이론으로부터 잘 알려진 사실의 특별한 경우로 $GF(2^m)$상의 (m, k) 타입의 Gauss 주기가 자기쌍대라는 명제의 필요충분조건은 k가 짝수일 때이다 라는 것이 [3]에서 증명되었다. 다음 보조정리는 특별한 경우의 기본적인 증명을 제공한다.

보조정리 1. $GF(2^m)$상의 타입 II ONB $\{\alpha^{2^s} | 0 \le s \le m-1\}$가 존재한다면 그것은 자기쌍대기저이다.

증명. 기저 원소의 치환 후, ONB는 $\{\beta^s+\beta^{-s} | 1 \le s \le m\}$이라 쓸 수 있다. $Tr((\beta^i+\beta^{-i})(\beta^j+\beta^{-j})) = Tr(\beta^{i-j}+\beta^{-(i-j)}+\beta^{i+j}+\beta^{-(i+j)})$임에 유의하자. 만약 $i=j$이면 임의의 $0 \le s \le m-1$에 대해 $Tr(\beta^{2i}+\beta^{-2i}) = Tr(\alpha^{2^s})$이다. 그러므로 대각합(trace)은 선형 독립이므로 $\alpha+\alpha^2+\cdots+\alpha^{2^{m-1}}=1$이다. $i \neq j$을 고려할 때, $i-j<0$이면 $i-j$을 $|i-j|$으로 바뀌고, $m+1 \le i+j \le 2m$이면 $i+j$은 $2m+1-(i+j)$으로 바뀐다 $(\beta^{2m+1}=1)$. 따라서, 임의의 $1 \le u, v \le m$에 대해, $Tr((\beta^i+\beta^{-i})(\beta^j+\beta^{-j})) = Tr(\beta^u+\beta^{-u}+\beta^v+\beta^{-v}) = Tr(\beta^u+\beta^{-u})+Tr(\beta^v+\beta^{-v})$을 얻는다. $\beta^u+\beta^{-u}$, $\beta^v+\beta^{-v}$은 $\{\alpha^{2^s} | 0 \le s \le m-1\}$의 원소이므로, $Tr(\beta^u+\beta^{-u})+Tr(\beta^v+\beta^{-v})=1+1=0$이다.

Ⅲ. 곱셈 알고리즘

보조정리 1의 증명으로부터 $\alpha_s = \beta^s+\beta^{-s}$, $1 \le s \le m$라 정의하면, 많은 기호들이 간단하게 표시될 수 있음을 알 수 있다. 지금부터 $\{\alpha^{2^s} | 0 \le s \le m-1\}$이 $GF(2^m)$상의 타입 II ONB이고 $\{\alpha_s | \alpha_s = \beta^s+\beta^{-s}, 1 \le s \le m\}$은 정규기저의 기저 원소들의 치환 후에 얻어진 기저라 하자. 주어진 $x = \sum_{i=1}^m x_i\alpha_i$, $x_i \in GF(2)$에 대해 보조정리 1을 이용하면,

$$x_s = \sum_{i=1}^m x_i\, Tr(\alpha_s\alpha_i) = Tr\left(\alpha_s \sum_{i=1}^m x_i\alpha_i\right) = Tr(\alpha_s x), \quad 1 \le s \le m$$

이다. 모든 정수 s에 대해, α_s와 x_s의 정의를 다음과 같이 확장한다.

정의 4. β를 $GF(2^{2m})$상에서 $p(=2m+1)$번째 원시근이라 하고, $x \in GF(2^m)$라 하자. 각각의 정수 s에 대해 α_s와 x_s는

$$\alpha_s = \beta^s+\beta^{-s}, \quad x_s = Tr(\alpha_s x)$$

으로 정의한다.

보조정리 2. $2m+1$이 s를 나누면 $\alpha_s = 0 = x_s$이다. 또한, 모든 s에 대해,

$$\alpha_{2m+1+s} = \alpha_s = \alpha_{2m+1-s} = \alpha_{-s}$$

이고

$$x_{2m+1+s} = x_s = x_{2m+1-s} = x_{-s}$$

이다.

증명. $\beta^s = \beta^{-s}$일 때만 $\alpha_s = \beta^s+\beta^{-s} = 0$이다. 즉, $\beta^{2s}=1$이다. 그리고 β는 p번째 원시근이므로 $2m+1=p$가 s를 나눌 때 나타난다. $\beta^{2m+1}=1$이므로 $\alpha_{2m+1+s} = \beta^{2m+1+s}+\beta^{-(2m+1+s)} = \beta^s+\beta^{-s} = \alpha_s$이다. 또한, $\alpha_{2m+1-s} = \beta^{2m+1-s}+\beta^{-(2m+1-s)} = \beta^{-s}+\beta = \alpha_s$이다. x_s의 결과는 α_s의 결과로부터 자명하게 얻는다.

임의의 정수 s, t에 대해,

$$\alpha_s\alpha_t = (\beta^s+\beta^{-s})(\beta^t+\beta^{-t}) = \alpha_{s-t}+\alpha_{s+t}$$

이다. 위의 식과 보조정리 2를 이용하여 다음 정리를 유도한다.

정리 2. $x = \sum_{i=1}^m x_i\alpha_i$, $y = \sum_{i=1}^m y_i\alpha_i$를 $GF(2^m)$의 원소라 하자. 그러면 $xy = \sum_{i=1}^m (xy)_i\alpha_i$이고 k번째 계수 $(xy)_k$는 다음을 만족한다.

$$(xy)_k = \sum_{i=1}^{2m} y_i x_{i-k} = \sum_{i=1}^{2m+1} y_i x_{i-k}.$$

증명. $GF(2^m)$상의 타입 II ONB의 자기쌍대성

(self duality)에 의해

$$\begin{aligned}(xy)_k &= Tr(\alpha_k xy)\\ &= Tr\left(\alpha_k x\sum_{i=1}^{m} y_i\alpha_i\right)=\sum_{i=1}^{m} y_i Tr(\alpha_k\alpha_i x)\\ &=\sum_{i=1}^{m} y_i Tr(\alpha_{i-k}x+\alpha_{i+k}x)\\ &=\sum_{i=1}^{m} y_i\left(Tr(\alpha_{i-k}x)+Tr(\alpha_{i+k}x)\right)\\ &=\sum_{i=1}^{m} y_i(x_{i-k}+x_{i+k})=\sum_{i=1}^{m} y_i x_{i-k}+\sum_{i=1}^{m} y_i x_{i+k}.\end{aligned}$$

반면에, 위 식의 두 번째 합은

$$\begin{aligned}\sum_{i=1}^{m} y_i x_{i+k} &= \sum_{i=1}^{m} y_{m+1-i}x_{m+1-i+k}\\ &=\sum_{i=1}^{m} y_{m+i}x_{m+i-k}\\ &=\sum_{i=m+1}^{2m} y_i x_{i-k}\end{aligned}$$

이고, 이 식의 첫 번째 등식은 합의 계수들의 재배열로부터 알 수 있고, 두 번째 등식은 보조정리 2로부터 알 수 있다. 그러므로,

$$(xy)_k=\sum_{i=1}^{m} y_i x_{i-k}+\sum_{i=1}^{m} y_i x_{i+k}=\sum_{i=1}^{2m} y_i x_{i-k}$$

을 얻는다. 보조정리 2에 의해 $y_{2m+1}=0$이므로, 위 결과로부터 $(xy)_k=\sum_{i=1}^{2m+1} y_i x_{i-k}$이다.

Ⅳ. 타입 II ONB를 이용한 비트 시리얼 구조

정리 2를 이용하여 $(xy)_k$을 행 벡터와 열 벡터의 행렬 곱으로 표현할 수 있다.

$$\begin{aligned}(xy)_k = &(x_{1-k}, x_{2-k}, \cdots, x_{2m-k}, x_{2m+1-k})\\ &\times(y_1, y_2, \cdots, y_{2m}, y_{2m+1})^T\end{aligned}$$

여기서, $(y_1, y_2, \cdots, y_{2m}, y_{2m+1})^T$은 행 벡터 $(y_1, y_2, \cdots, y_{2m}, y_{2m+1})$의 전치 행렬이다. 또한

$$\begin{aligned}(xy)_{k+1} = &(x_{-k}, x_{1-k}, \cdots, x_{2m-1-k}, x_{2m-k})\\ &\times(y_1, y_2, \cdots, y_{2m}, y_{2m+1})^T\end{aligned}$$

이다. 보조정리 2에 의해 $x_{-k}=x_{2m+1-k}$이므로, $(x_{-k}, x_{1-k}, \cdots, x_{2m-1-k}, x_{2m-k})$은 $(x_{1-k}, x_{2-k}, \cdots, x_{2m-k}, x_{2m+1-k})$을 오른쪽으로 한 자리 순환 이동한 것임을 안다. 이러한 결과로부터, 그림 1에서 나타낸 쉬프트 레지스트 구조에서 곱셈 알고리즘을 실행할 수 있다. 쉬프트 레지스트의 초기 입력값은 $(x_0, x_1, \cdots, x_{2m})=(0, x_1, \cdots, x_m, x_m, \cdots, x_1)$이다. k 클럭 사이클 후에 기저 $\{\alpha_1, \cdots, \alpha_m\}$에 대응되는 xy의 k번째 계수 $(xy)_k$를 얻는다. 타입 II ONB를 이용한 비트 패러럴 곱셈기는 [4]에서 논의되었다.

Ⅴ. 타입 II ONB를 이용한 시스톨릭 구조

5.1 비트 패러럴 어레이

기저 $\{\alpha_1, \alpha_2 \cdots, \alpha_m\}$은 앞 절의 Berlekamp 타입의 효율적인 비트 시리얼 곱셈기을 구현하기 위해 사용되었다. 기저 원소 α_i의 재사용으로 작은 지연시간과 낮은 복잡도의 비트 패러럴 시스톨릭 곱셈기를 만들 수 있다. 우선, $\{\alpha_1, \alpha_2, \alpha_3, \cdots, \alpha_m\}$과 $\{\alpha_1, \alpha_3, \alpha_5, \cdots, \alpha_{2m-1}\}$이 같은 집합임에 유의하자. 즉, m이 홀수이면 $\alpha_1, \alpha_3, \cdots, \alpha_{2m-1}$는 $\alpha_1, \alpha_3, \cdots, \alpha_m, \alpha_{m+2}=\alpha_{m-1}, \alpha_{m+4}=\alpha_{m-3}, \cdots, \alpha_{2m-1}=\alpha_2$이고 m이 짝수이면 $\alpha_1, \alpha_3, \cdots, \alpha_{m-1}, \alpha_{m+1}=\alpha_m$,

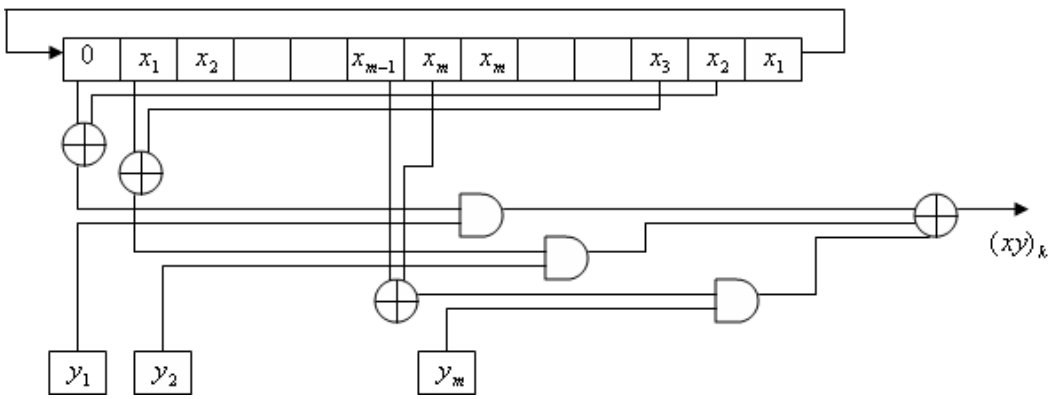

그림 1. 타입 II ONB를 이용한 비트 시리얼 곱셈

$\alpha_{m+3}=\alpha_{m-2},\cdots,\alpha_{2m-1}=\alpha_2$이다. 그러므로 $\{\alpha_1, \alpha_3, \alpha_5, \cdots, \alpha_{2m-1}\}$ 또한 $GF(2^m)$의 기저이고 $\{\alpha_1, \alpha_2, \alpha_3, \cdots, \alpha_m\}$으로부터 $\{\alpha_1, \alpha_3, \alpha_5, \cdots, \alpha_{2m-1}\}$의 기저 변환은 위에서 언급된 바와 같이 자명하다. $x=\sum_{i=1}^{m}x_i\alpha_i$를 $GF(2^m)$의 원소라 하자. 정의 4에서 임의의 정수 s에 대해 원소 $x_s\in GF(2)$은 $x_s = Tr(\alpha_s x)$으로 정의됨을 상기하자. $y=\sum_{i=1}^{m}y_i\alpha_i$을 $GF(2^m)$의 다른 원소라 하자. 각 정수 j에 대해, 행 벡터 X_j, Y_j는

$$X_j=(x_j, x_{j+1}, \cdots, x_{j+2m}),\quad Y_j=(y_j, y_{j+1}, \cdots, y_{j+2m})$$

으로 정의된다. 음이 아닌 정수 s에 대해, X_{j+s}, Y_{j+s}은 X_j, Y_j을 각각 왼쪽으로 s만큼 순환 이동한 것임을 유의하자. 또한, X_{j-s}, Y_{j-s}은 X_j, Y_j을 오른쪽으로 s만큼 순환 이동한 것이다. 게다가 정리 2의 사용으로 임의의 j, k에 대해, 다음 식을 얻는다.

$$\begin{aligned}(xy)_k&=\sum_{i=1}^{2m+1}y_ix_{i-k}=X_{1-k}Y_1^T\\&=(x_{1-k}, x_{2-k}, \cdots, x_{2m+1-k})\\&\quad\times(y_1, y_2, \cdots, y_{2m+1})^T\\&=(x_{j-k}, x_{j+1-k}, \cdots, x_{j+2m-k})\\&\quad\times(y_j, y_{j+1}, \cdots, y_{j+2m})^T\\&=X_{j-k}{Y_j}^T\end{aligned}.$$

정리 3. $x=\sum_{i=1}^{m}x_i\alpha_i$, $y=\sum_{i=1}^{m}y_i\alpha_i$를 $GF(2^m)$의 원소라 하자. 그러면

$$(xy)_{2k-1}=\sum_{i=1}^{m}(y_{i+k-1}x_{i-k}+y_{i-k}x_{i+k-1})+y_{m+1-k}x_{m+1-k}$$

을 얻는다.

증명. 정리 3의 설명 바로 전의 내용에 의해,

$$\begin{aligned}(xy)_{2k-1}&=X_{k-(2k-1)}{Y_k}^T=X_{1-k}Y_k^T\\&=(x_{1-k}, x_{2-k}, \cdots, x_{2m+1-k})\\&\quad\times(y_k, y_{k+1}, \cdots, y_{k+2m})^T\\&=\sum_{i=1}^{2m+1}y_{i+k-1}x_{i-k}\\&=\sum_{i=1}^{m}y_{i+k-1}x_{i-k}+y_{m+k}x_{m+1-k}\\&\quad+\sum_{i=m+2}^{2m+1}y_{i+k-1}x_{i-k}\\&=\sum_{i=1}^{m}y_{i+k-1}x_{i-k}+y_{m+1-k}x_{m+1-k}\\&\quad+\sum_{i=m+2}^{2m+1}y_{i+k-1}x_{i-k}\end{aligned}$$

이다. 반면에 위 식의 두 번째 합은

$$\begin{aligned}\sum_{i=m+2}^{2m+1}y_{i+k-1}x_{i-k}&=\sum_{i=1}^{m}y_{2m+2-i+k-1}x_{2m+2-i-k}\\&=\sum_{i=1}^{m}y_{i-k}x_{i+k-1}\end{aligned}$$

이고, 여기서 첫 번째 등식은 합의 계수의 재배열로부터 알 수 있고, 두 번째 등식은 보조정리 2로부터 알 수 있다. 그러므로 원하는 결과

$$\begin{aligned}(xy)_{2k-1}&=\sum_{i=1}^{m}y_{i+k-1}x_{i-k}+y_{m+1-k}x_{m+1-k}\\&\quad+\sum_{i=1}^{m}y_{i-k}x_{i+k-1}\end{aligned}$$

을 얻는다.

지금부터 각 $(xy)_{2k-1}$에 대해, 열 벡터를

$$W_k=(w_{1k}, w_{2k}, \cdots, w_{mk}, w_{(m+1)k})^T,$$

라 정의하자. 여기서

$$\begin{aligned}w_{ik}&=y_{i+k-1}x_{i-k}+y_{i-k}x_{i+k-1}, &&\text{if } 1\le i\le m\\w_{(m+1)k}&=y_{m+1-k}x_{m+1-k}, &&\text{if } i=m+1\end{aligned}$$

이다. 그러면 열 벡터 W_k의 모든 성분의 합은 정확히 $(xy)_{2k-1}$이고 W_k은 $(m+1)\times m$ 행렬 $W=(w_{ik})$의 k번째 열 벡터로 나타난다. 여기서 행렬 W는

$$W=\begin{pmatrix}w_{11}&w_{12}&w_{13}&\cdots&w_{1m}\\w_{21}&w_{22}&w_{23}&\cdots&w_{2m}\\w_{31}&w_{32}&w_{33}&\cdots&w_{3m}\\\vdots&\vdots&\vdots&\ddots&\vdots\\w_{m1}&w_{m2}&w_{m3}&\cdots&w_{mm}\\w_{(m+1)1}&w_{(m+1)2}&w_{(m+1)3}&\cdots&w_{(m+1)m}\end{pmatrix}$$

이다. 각 $1\le i, k\le m$에 대해, 다음 관계식

$$w_{ik}=y_{i+k-1}x_{i-k}+y_{i-k}x_{i+k-1}$$

을 이용하여 다음 식

$$w_{(i-1)(k-1)}=y_{i+k-3}x_{i-k}+y_{i-k}x_{i+k-3}$$

을 얻는다. 즉, w_{ik}의 식에서 신호 x_{i-k}, y_{i-k}은 $w_{(i-1)(k-1)}$의 식의 신호로부터 얻는다. 또한,

$$w_{(i-1)(k+1)}=y_{i+k-1}x_{i-k-2}+y_{i-k-2}x_{i+k-1}$$

이므로, w_{ik}의 식에서 신호 x_{i+k-1}, y_{i+k-1}은 $w_{(i-1)(k+1)}$의 식의 신호로부터 얻는다. 게다가 마지막 열의 신호는 m번째 열의 신호로부터 얻는다. 즉, $w_{(m+1)1}=y_m x_m$은 식 $w_{m1}=y_m x_{m-1}+y_{m-1}x_m$의 신호 y_m, x_m으로부터 얻는다. 그리고, 각 $2\le k\le m$에 대해, 식 $w_{(m+1)k}=y_{m+1-k}x_{m+1-k}$은 식 $w_{m(k-1)}=y_{m+k-2}x_{m+1-k}+y_{m+1-k}x_{m+k-2}$의 신호 y_{m+1-k}, x_{m+1-k}으로부터 얻는다. 이 결과로부터 기저 $\{\alpha_1,\alpha_3,\cdots,\alpha_{2m-1}\}$에 대응하는 비트 패러럴 시스톨릭 곱셈기를 설계할 것이다. 기본 셀의 회로는 그림 2에 설명되었으며, 그림에서 •은 1-비트 래치(플립-플롭)이다. 수직선의 출력은 곱의 부분합으로 산출된다.

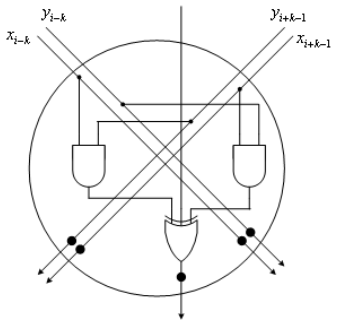

그림 2. (i, k)번째 기본 셀의 회로도

편의상 타입 II ONB의 존재성이 잘 알려진 m=5에 대해 고려하자. 그러면 행렬 W는

$$W=\begin{pmatrix} y_1x_0+y_0x_1 & y_2x_1+y_1x_2 & y_3x_2+y_2x_3 & y_4x_3+y_3x_4 & y_5x_4+y_4x_5 \\ y_2x_1+y_1x_2 & y_3x_0+y_0x_3 & y_4x_1+y_1x_4 & y_5x_2+y_2x_5 & y_5x_3+y_3x_5 \\ y_3x_2+y_2x_3 & y_4x_1+y_1x_4 & y_5x_0+y_0x_5 & y_5x_1+y_1x_5 & y_4x_2+y_2x_4 \\ y_4x_3+y_3x_4 & y_5x_2+y_2x_5 & y_5x_1+y_1x_5 & y_4x_0+y_0x_4 & y_3x_1+y_1x_3 \\ y_5x_4+y_4x_5 & y_5x_3+y_3x_5 & y_4x_2+y_2x_4 & y_3x_1+y_1x_3 & y_2x_0+y_0x_2 \\ y_5x_5 & y_4x_4 & y_3x_3 & y_2x_2 & y_1x_1 \end{pmatrix}$$

이고, 여기서 $1\le i,\ k\le m$에 대해, $w_{ik}=y_{i+k-1}x_{i-k}+y_{i-k}x_{i+k-1}$이다. $z=\sum_{i=1}^{m} z_i\alpha_i$를 $GF(2^m)$의 또 다른 원소라 하고, 그림 3에서 나타난 비트 패러럴 시스톨릭 구조는 연산 $u=xy+z$를 실행하는 것이다. 이 구조에서 $x_0=0=y_0$이고 k번째 열의 출력값은 u_{2k-1}임에 유의하자.

표 1에서는 제안된 곱셈기와 다른 비트 패러럴 시스톨릭 곱셈기를 비교한다. [9]의 곱셈기는 쌍대기저를 사용하므로 그것은 기저 변환 과정이 필요하다. 표 1에서 알 수 있듯이 제안된 곱셈기는 [10]의 곱셈기를 제외하고 가장 좋은 하드웨어 복잡도와 지연시간을 가짐을 보였다. [10]의 곱셈기는 AOP 기저가 존재할 때 유한체 $GF(2^m)$에 적용된다.

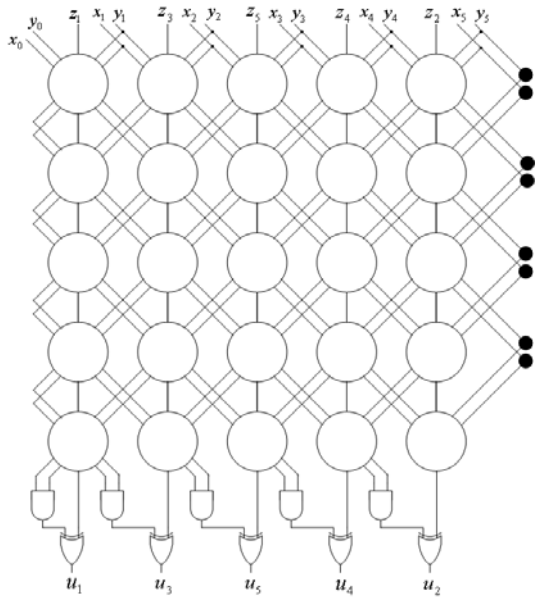

그림 3. $GF(2^5)$상의 $u=xy+z$을 계산하기 위한 시스톨릭 구조

표 1. 비트 패러럴 시스톨릭 어레이 비교

	Wang[7]	Yeh[8]	Fenn[9]	Wei[11]	Lee[10]	그림 3
기저	다항식	다항식	쌍대	다항식	AOP	타입 II ONB
함수	AB	$AB+C$	AB	AB^2+C	$AB+C$	$AB+C$
셀 복잡도						
AND	2	2	2	3	1	2
XOR	0	2	2	1	1	0
3XOR	1	0	0	1	0	1
Latch	7	7	7	10	3	5
셀의 개수	m^2	m^2	m^2	m^2	$(m+1)^2$	m^2
지연시간	$3m$	$3m$	$3m$	$3m$	$m+1$	$m+1$
최대처리 지연시간	$D_A+D_{3X}+D_L$	$D_A+D_X+D_L$	$D_A+D_X+D_L$	$D_A+D_{3X}+D_L$	$D_A+D_X+D_L$	$D_A+D_{3X}+D_L$

이 때, 다항식 $1+x+x^2+\cdots+x^m \in GF(2)[x]$를 차수 m인 AOP라 부른다. 유한체 $GF(2^m)$은 차수 m인 AOP가 $GF(2)$상의 기약 다항식일 때 AOP 기저를 가진다. AOP 기저가 $GF(2^m)$상에 존재한다는 명제의 필요충분조건은 $m+1=p$가 소수이고 2가 (mod p)에 대한 원시근이다 라는 것을 보이는 것은 어렵지 않다. 적당히 작은 값 m에 대한 AOP 기저의 존재성은 잘 알려져 있다. 사실, [6, p. 100]의 표에서 AOP 기저가 존재하는 2000보다 작은 m의 개수는 겨우 118개이다. 예를 들어, m=2, 4, 10, 12, 18, 28, 36, 52, 58, 60, 66, 82, 100, 106, …일 때 AOP 기저를 가진다. 반면에 같은 표에서 타입 II ONB가 존재하는 2000보다 작은 m의 개수는 324개이다. m=2, 3, 5, 6, 9, 11, 14, 18, 23, 26, 29, 30, 33, 35, 39, 41, 50, 51, 53, 65, 69, 74, …일 때 타입 II ONB가 존재한다. 그러므로 그림 3에서 제안된 곱셈기는 AOP 기저를 사용한 곱셈기보다 더 많은 경우의 m에 적용되어진다.

5.2 선형 시스톨릭 어레이

그림 3은 패러럴-인-패러럴-아웃 구조로 $xy+z$를 계산하기 위한 (양방향) 선형 시스톨릭 어레이를 구현하기 위해 약간 변형될 수 있다. 그림 4는 $i(1\le i\le m+1)$번째 클럭 사이클 전의 $k(1\le k\le m)$번째 기본 셀의 구조를 나타낸다. 부분합에 대한 플립-플롭은 $s_{ik}=z_{2k-1}+\sum_{j=1}^{i-1}(y_{i+k-1}x_{i-k}+y_{i-k}x_{i+k+1})$값을 가진다. 특히 초기에 z_{2k-1}으로 시작한다. $y_{m+1-k}x_{m+1-k}$의 마지막 덧셈을 제어하기 위해 01…11의 m개의 논리값을 가지는 제어 신호를 사용한다. x_{i-k}, $y_{i-k}(i=1, 1\le k\le m)$의 초기값은 x_0, x_1, …, x_{m-1}과 y_0, y_1, …, y_{m-1}이다. 또한, x_{i+k-1}, $y_{i+k-1}(i=1, 1\le k\le m)$의 초기값은 x_1, x_2, …, x_m과 y_1, y_2, …, y_m이다. 제안된 구조의 지연시간은 $m+1$이고 처리율은 $1/(m+1)$이다.

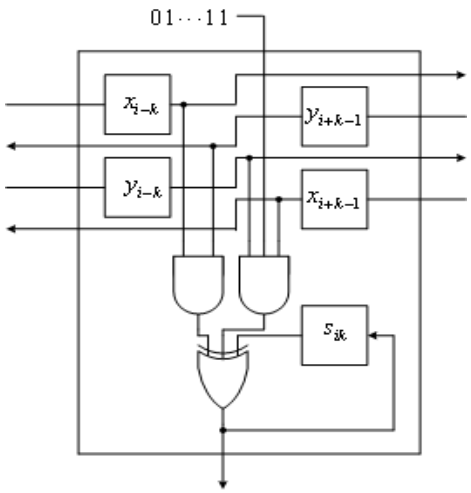

그림 4. $GF(2^m)$에서 $u=xy+z$를 계산하기 위한 $i(1\le i\le m+1)$번째 클럭 사이클 전의 k번째 기본 셀

Ⅵ. 결 론

본 논문에서는 타입 II ONB를 이용한 비트 패러럴, 시리얼 시스톨릭 곱셈기를 제안했다. 표 1에서 제안된 곱셈기는 AOP 기저를 사용한 [10]에서 제안된 곱셈기를 제외한 다른 곱셈기보다 낮은 복잡도와 지연시간을 가짐을 보였다. 그러나 AOP 기저는 타입 II ONB보다 작은 빈도로 나타난다. [6, p. 100]의 표에서 타입 II ONB는 AOP 기저보다 3배 더 존재한다는 것을 알 수 있다. 그러므로 제안된 비트 패러럴 시스톨릭 곱셈기는 AOP 기저가 존재하지 않거나 다른 낮은 복잡도의 시스톨릭 구조가 아직 알려지지 않은 많은 유한체에 대해 효율적인 하드웨어 구조를 제공한다. 또한, 그림 3의 구조는 그림 5에 나타난 선형(1차원) 시스톨릭 어레이를 구현하기 위해 수직 방향으로 사영을 통해서 쉽게 변형할 수 있다. 이 경우에 제안된 선형 시스톨릭 어레이는 패러럴-인-패러럴-아웃 구조이고 $m+1$ 클럭 사이클 후에 출력한다. 표 2의 비교로부터 제안된

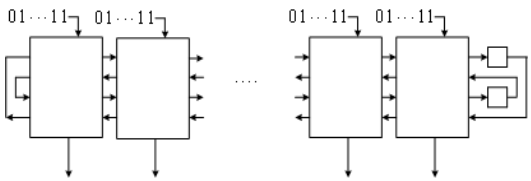

그림 5. 제안된 선형 시스톨릭 어레이

표 2. 제안된 선형 시스톨릭 어레이와 다른 비트 시리얼 시스톨릭 곱셈기 비교

	Wang[7]	Yeh[8]	Fenn[9]	그림 4
기저	다항식	다항식	쌍대	타입 II ONB
AND	3	3	3	3
XOR	0	2	2	0
3XOR	1	0	0	1
MUX	2	2	3	0
flip-flop(Latch)	10	12	10	5
셀의 개수	m	m	m	m
지연시간	$3m$	$3m$	$3m$	$m+1$
최대처리 지연시간	D_A+D_{3X} $+D_L+D_M$	D_A+D_X $+D_L+D_M$	D_A+D_X $+D_L+D_M$	$2D_A+D_{3X}$ $+D_L$
처리량	$1/m$	$1/m$	$1/m$	$1/(m+1)$

선형 시스톨릭 어레이가 공간 복잡도와 지연 시간을 줄임을 알 수 있다.

참 고 문 헌

〔1〕 E.R. Berlekamp, "Bit-serial Reed-Solomon encoders," *IEEE Trans. Inform. Theory*, vol. 28, pp. 869-874, 1982.

〔2〕 M. Wang and I.F. Blake, "Bit serial multiplication in finite fields," *SIAM J. Disc. Math.*, vol. 3, pp. 140-148, 1990.

〔3〕 S. Gao, J. von zur Gathen and D. Panario, "Gauss periods and fast exponentiation in finite fields," *Lecture Notes in Computer Science*, vol. 911, pp. 311-322, 1995.

〔4〕 B. Sunar and C.K. Koc, "An efficient optimal normal basis type II multiplier," *IEEE Trans. Computers*, vol 50, pp. 83-87, 2001.

〔5〕 A. Reyhani-Masoleh and M.A. Hasan, "A new construction of Massey-Omura parallel multiplier over $GF(2^m)$," *IEEE Trans. Computers*, vol. 51, pp. 511-520, 2002.

〔6〕 A.J. Menezes, *Applications of finite fields*, Kluwer Academic Publisher, 1993.

〔7〕 C.L. Wang and J.L. Lin, "Systolic array implementation of multipliers for finite fields $GF(2^m)$," *IEEE Trans. Circuits Syst.*, vol. 38, pp. 796-800, 1991.

〔8〕 C.S. Yeh, I.S. Reed and T.K. Troung, "Systolic multipliers for finite fields $GF(2^m)$," *IEEE Trans. Computers*, vol. C-33, pp. 357-360, 1984.

〔9〕 S.T.J. Fenn, M. Benaissa and D. Taylor, "Dual basis systolic multipliers for $GF(2^m)$," *IEE Proc. Comput. Digit. Tech.*, vol. 144, pp. 43-46, 1997.

〔10〕 C.Y. Lee, E.H. Lu and J.Y. Lee, "Bit parallel systolic multipliers for $GF(2^m)$ fields defined by all one and equally spaced polynomials," *IEEE Trans. Computers*, vol. 50, pp. 385-393, 2001.

〔11〕 C.W. Wei, "A systolic power sum circuit for $GF(2^m)$," *IEEE Trans. Computer*, vol. 43, pp. 226-229, 1994.

〔12〕 S.K. Jain, L. Song and K.K. Parhi, "Efficient semisystolci architectures for finite field arithmetic," *IEEE Trans. VLSI Syst.*, vol. 6, pp. 101-113, 1998.

〔13〕 J.H. Guo and C.L. Wang, "Systolic array implementation of Euclid's algorithm for inversion and division in $GF(2^m)$," *IEEE Trans. Computers*, vol. 47, pp. 1161-1167, 1998.

〔14〕 S. Kwon and H. Ryu, "Efficient bit serial multiplication using optimal normal bases of type II in $GF(2^m)$," *Lecture Notes in Computer Science*, vol. 2433, pp. 300-308, 2002.

〔15〕 C.Y. Lee, E.H. Lu and L.F. Sun, "Low complexity bit parallel systolic architecture for computing AB^2+C in a class of finite field $GF(2^m)$," *IEEE Trans. Circuits Syst. II*, vol. 48, pp. 519-523, 2001.

〔16〕 W.C. Tsai, C.B. Shung and S.J. Wang, "Two systolic architectures for modular multiplication," *IEEE Trans. VLSI Syst.*, vol. 8, pp. 103-107, 2000.

〔17〕 T. Itoh and S. Tsujii, "Sturcture of parallel multipliers for a class of finite fields $GF(2^m)$," *Information and computation*, vol. 83, pp. 21-40, 1989.

〔18〕 C.K. Koc and B. Sunar, "Low complexity bit paraller canonical and normal basis multipliers for a class of finite fields," *IEEE Trans. Computers*, vol. 47, pp. 353-356, 1998.

〔19〕 C. Paar, P. Fleischmann and P. Roelse, "Efficient multiplier architectures for Galois fields $GF(2^{4n})$," *IEEE Trans. Computers*, vol. 47, pp. 162-170, 1998.

〔20〕 H. Wu, M.A. Hasan, I.F. Blake and S. Gau, "Finite field multiplier using redundant representation," *IEEE Trans. Computers*, vol. 51, pp. 1306-1316, 2002.

〔21〕 G.B. Agnew, R.C. Mullin, I. Onyszchuk and S.A. Vanstone, "An implementation for a fast public key cryptosystem," *J. Cryptology*, vol. 3, pp. 63-79, 1991.

권 순 학 (Soonhak Kwon) 정회원

1990년 2월 KAIST 수학과 (학사)
1992년 2월 서울대학교 수학과 (석사)
1997년 5월 Johns Hopkins University (박사)
1998년 3월~현재 성균관대학교 수학과, 부교수

<관심분야> 정수론, 암호론, Cryptographic Hardware, USN 보안

권 윤 기 (Yun Ki Kwon) 준회원

2001년 2월 대진대학교 수학과 (학사)
2003년 8월 성균관대학교 수학과 (석사)
2003년 9월~현재 성균관대학교 수학과 박사과정

<관심분야> 공개키 암호시스템, 암호시스템 구현, 타원곡선 암호시스템, Pairing 기반 암호시스템, USN 보안

김 창 훈 (Chang Hoon Kim) 정회원

2001년 2월 대구대학교 컴퓨터정보공학부 (학사)
2003년 2월 대구대학교 컴퓨터정보공학과 (석사)
2006년 8월 대구대학교 컴퓨터정보공학과 (박사)
2006년 9월 대구대학교 정보통신공학부 BK21 연구교수
2007년 8월~현재 대구대학교 컴퓨터IT공학부, 전임강사

<관심분야> 암호 시스템, Embedded System, RFID/USN 보안

홍 춘 표 (Chun Pyo Hong) 정회원

1978년 2월 경북대학교 전자공학과 (학사)
1986년 12월 Georgia Institute of Technology ECE (석사)
1991년 12월 Georgia Institute of Technology ECE (박사)
1994년 9월~현재 대구대학교 정보통신공학부 교수

<관심분야> DSP 하드웨어 및 소프트웨어, 컴퓨터 구조, VLSI 신호처리, Embedded System